Comments of the Messaging Malware Mobile Anti-Abuse Working Group (M^{3}AAWG) on NIST SP 800-218A, Secure Software Development Practices for Generative AI and Dual-Use Foundation Models

Consultation reference: NIST SP 800-218A, Secure Software Development Practices for Generative AI and Dual-Use Foundation Models

The Messaging Malware Mobile Anti-Abuse Working Group (M^{3}AAWG) appreciates the opportunity to submit comments in response to the above-referenced consultation. M^{3}AAWG is a technology-neutral global industry association. As a working body, we focus on operational issues of internet abuse including technology, industry collaboration, and public policy. With more than 200 institutional members worldwide, we bring together stakeholders in the online community in a confidential yet open forum, developing best practices and cooperative approaches for fighting online abuse.

The increasing importance of secure development of software and AI systems carries specific risks associated with the abuse of AI systems and AI tools used in software development. As a group of anti-abuse specialists, M^{3}AAWG thus welcomes the opportunity to comment on the current version of NIST SP 800-218A:

1. We note numerous references to the software development life cycle (SDLC) in the document. M^{3}AAWG suggests framing this document as providing input into an Artificial Intelligence Development Life Cycle[1] (AILC). This would emphasize the different and additional steps in the AI development process.

2. Going forward, we recommend further guidance on the use of AI as a tool *within* the software development life cycle, its associated risks and apposite mitigations.

3. The current draft does not consider in depth the large-scale impact of AI systems on organizations, people, society, and on overall system architecture. These aspects should be considered as part of an Artificial Intelligence Development Life Cycle. While the document focus is not to provide in-depth guidance on these questions, setting the context with an informative note would front-load such considerations within the development life cycle.

[1] See https://coe.gsa.gov/coe/ai-guide-for-government/understanding-managing-ai-lifecycle

4. As a large majority of organizations will not be able or willing to develop their own AI models or systems, external or partly external AI system supply chains as well as external development will be common. More detail on the management of supply chains in AI development and AI-enabled software development, either in this or in another document, is essential.
    a. A key consideration to address might be the way in which the recommendations provided would be considered and implemented. Would they be focused only on supply chains, on the resulting products, or a combination thereof?
    b. Another important and timely aspect to cover would be the management of AI-enabled coding tools and their impact on developers and the SDLC.

We appreciate the opportunity to submit these comments, and we welcome further opportunities to engage as needed to answer any questions during this process. Please address any inquiries to M^{3}AAWG Executive Director Amy Cadagin at comments@m3aawg.org.

Sincerely,
Amy Cadagin, Executive Director
Messaging Malware Mobile Anti-Abuse Working Group
comments@m3aawg.org
P.O. Box 9125 Brea, CA 92822